

REMARKS

The above amendments to the above-captioned application along with the following remarks are being submitted as a full and complete response to the Official Action dated May 12, 2005. In view of the above amendments and the following remarks, the Examiner is respectfully requested to give due consideration to this application, to indicate the allowability of the claims, and to pass this case to issue.

Status of the Claims

Claims 1, 3-5 and 7-8 are under consideration in this application. Claims 2, 6, and 9-12 are being cancelled without prejudice or disclaimer. Claims 1 and 5 are being amended, as set forth in the above marked-up presentation of the claim amendments, in order to more particularly define and distinctly claim applicant's invention.

The claims are being amended to correct formal errors and/or to better recite or describe the features of the present invention as claimed. All the amendments to the claims are supported by the specification. Applicant hereby submits that no new matter is being introduced into the application through the submission of this response.

Prior Art Rejections

Under 35 U.S.C. §103(a), the Examiner rejected claims 1 and 4 as being obvious over US Patent No. 6,219,791 to Blanchard et al. (hereinafter "Blanchard") in view of the article "On the Importance of Checking Cryptographic Protocols for Faults" to Boneth et al. (hereinafter "Boneth"); claim 2 as being obvious over Blanchard and Boneth in view of the article "Concurrent Error Detection In Block Ciphers" to Fernandez-Gomez et al. (hereinafter "Fernandez-Gomez"); claim 3 over Blanchard and Boneth in view of US Application No. 2002/0178354 A1 to Ogg et al. (hereinafter "Ogg"); claims 5-6 and 8 over US Patent No. 5,991,401 to Daniels et al. (hereinafter "Daniels") in view of Boneth and Fernandez-Gomez; claim 7 over Daniels in view of Fernandez-Gomez and Ogg; claim 8 over Daniels in view of Fernandez-Gomez, Boneth and Ogg; claims 9-10 and 12 over Daniels in view of the publication "Applied Cryptography" to Schneier (hereinafter "Schneier") and Boneth; and claim 11 over Daniels in view of Schneier, Boneth and Ogg. These rejections have been carefully considered, but are most respectfully traversed.

The tamper-resistant fault detection method (e.g., Fig. 5; pp. 14-15) for an IC card 101 (Fig. 1; p. 1, lines 5-6) including an information processing device 102 mounted thereon

(e.g., a chip including a CPU therein; p. 1, lines 22-23; Abstract; “*A tamper-resistant apparatus represented by an IC card chip comprises a storage device having a program-storage portion which stores programs and a data-storage portion which stores data, and a central processing unit (CPU) which performs data processing by executing designated processes following the programs. The apparatus can be understood as an information processing device in which the programs, composed of processing instructions giving execution orders to the CPU, provide one or more data processing mean*” p. 6, lines 10-19), as now recited in claim 1, comprises the steps of: (1) performing a DES (data encryption standard) symmetric-key encryption process $Z = E(M, K)$ (p. 11, lines 16-17) in which a secret key K is to be applied to an input plaintext M , and storing a processing result Z in a memory 204 in the IC card 101 (Fig. 2); (2) performing a corresponding DES decryption process $W = D(Z, K)$ for said process result Z stored on said memory 204 and storing the decryption result W on the memory 204; (3) outputting said processing result Z from said information processing device when said processing result W coincides with said plaintext M ($W=M$) ; and (4) suppressing the output of said processing result Z from said information processing device when said processing result W does not coincide with said plaintext M ($W \neq M$).

The main purpose of the present invention is to prevent an attack on an encryption mechanism from successfully occurring so as to prevent an attacker's attempt to obtain the information of how the encryption mechanism processes data by acquiring both an incorrect result and a correct answer. For this purpose, the present invention is configured in such a manner that it prohibits the processing result from outputting out of the mechanism when the result proves incorrect (p.13, line 12 to p. 14, line 5, in particular, p.14, lines 4-5). If any error occurs caused by an erroneous operation in the DES processing result generated by an attacker while an IC card is performing encryption processing (p. 4, lines 1-3), the error is surely detected by the observation of the decryption result such that the IC card get reset to suppress outputting of the processing result Z . As such, an attacker is not able to obtain any erroneous processing result which is necessary for an attack to execute an attack (p. 15, lines 11-17).

The invention, as now recited in claim 5, is directed to a tamper-resistant fault detection method (e.g., Fig. 6; pp. 15-16) for an IC card including an information processing device mounted thereon, that comprises the steps of: (1) performing a DES (data encryption standard) symmetric-key encryption process $Z = D(C, K)$ wherein a secret key K is to be

applied to an input ciphertext C, and storing the processing result Z on a memory in the IC card; (2) performing a corresponding DES encryption process $W = E(Z, K)$ for the processing result Z stored on said memory, and storing the result W on the memory; (3) outputting said processing result Z from said information processing device when said processing result W coincides with said ciphertext C ($W=C$); and (4) suppressing the output of said processing result Z from said information processing device when said processing result W does not coincide with said ciphertext C ($W \neq C$).

Applicants respectfully contend that none of the cited prior art references teaches or suggests such a tamper-resistant fault detection method for an IC card including the steps of “performing a DES symmetric-key encryption process in which a secret key K is to be applied to an input plaintext M, and storing a processing result Z in a memory in the IC card; (2) performing a corresponding DES decryption process $W = D(Z, K)$ for said process result Z stored on said memory 204 and storing the decryption result W on the memory 204; (3) outputting said processing result Z from said information processing device mounted on the IC card when said processing result W coincides with said plaintext M; and (4) suppressing the output of said processing result Z from said information processing device when said processing result W does not coincide with said plaintext M” as does the invention.

As admitted by the Examiner, Blanchard does not disclose an IC card performing the method of claim 1 to verify a cryptographic process (p. 4, lines 8-9 of the outstanding Office Action). Blanchard produces a data packet consisting of a plaintext M and an error detection data added thereto (FIG. 4, step 410). In Blanchard's step 410, an error detection data is added to the plaintext M. Then, Blanchard encrypts the data packet (step 420), and he decrypts the encrypted data packet (step 430). The decrypted data packet is expected to contain both the plaintext M and the error detection data. Blanchard judges whether there is an error on the decrypted data packet by using just the error detection data (step 450 and 460; col. 4, line 63 - col. 5, line 1), rather than comparing the decrypted data W with the plaintext M as the present invention.

Contrary to the Examiner's assertion that Blanchard "outputs said processing result z from said information processing device when said processing result W coincides with said plaintext M (Fig. 4, step 470)"; Blanchard suggests nothing more than judging whether there is an error in the decrypted data W in the light of the error detection data.

Boneh was relied upon by the Examiner to compensate for Blanchard's deficiencies. However, Boneh merely discloses a signature technique using RSA algorithm, not related to

DES. Further, the relevant portion of Boneh (p.37, last par.; p. 38, 4th par.) cited by the Examiner neither disclose a specific verifying means nor disclose a step of comparing the result W with the plaintext M as does the present invention.

RSA adopts an asymmetric-key, which means that encryption process followed by decryption process or vice versa need both a secret key and a public key. However, it is difficult for outsiders to guess the public key from the secret key. The operation of obtaining the public key from the secret key requires secret prime numbers p and q as well as its reverse operation does. In usual RSA cryptography which does not utilize CRT (Chinese remainder theorem), since the secret prime numbers p and q are unnecessary, even someone who owns a secret key does not frequently have its public key nearby. Yet users have to explicitly give a public key for RSA input data. On the other hand, in DES cryptography using symmetric keys, this situation does not occur because both encryption and decryption use the same key. Hence, DES is a technology totally different from RSA in its algorithm. Boneh simply does not perform a DES symmetric-key encryption process $Z = E(M, K)$ and then a corresponding DES decryption process $W = D(Z, K)$ with the same secret key K .

Even if, arguendo, Boneh's encrypted message $E = M^d \bmod N$ were analogous to $Z = E(M, K)$, Boneh merely checks whether the signature/output $E (\sim Z)$ was correct (p. 38, 4th full paragraph; "check the output of the computation before releasing it" p. 49, the paragraph starts with "one can envision..."), rather than comparing the message M with any decrypted message $W = E^d \bmod N (W=M?)$.

As admitted by the Examiner, Blanchard does not disclose using DES algorithm (p. 4, last paragraph of the outstanding Office Action) such that Fernandez-Gomez was cited to compensate for the deficiencies of the combination of Blanchard and Boneh. Although Fernandez-Gomez encrypts a plain text into a cipher text, decrypts the cipher text, and then compares the decrypted text with the original plain text (Fig. 7), it, however, does not output the cipher text Z itself as the processing result, because it intends to detect hardware failures of the cipher mechanism (p. 979, right col., line 11; p. 980, left col., line 4-). As Fernandez-Gomez only intends to gather an error detection probability to see if how many errors are detected on the cipher mechanism, it does not output the cipher text Z gained as a processing result to the external world. Hence, Fernandez-Gomez fails to teach the present invention in how to control the output of the processing result Z and how to output it when it is correct. In other words, Fernandez-Gomez neither (i) output said processing result Z from said information processing device when said processing result W coincides with said plaintext M

($W=M$); nor (ii) suppress the output of said processing result Z from said information processing device when said processing result W does not coincide with said plaintext M ($W \neq M$).

Other cited references fail to compensate for the above-mentioned deficiencies in terms of the independent claims as well as the dependant claims as discussed as follows. In particular, Daniels (Fig. 3) decrypts an encrypted packet by utilizing a master decryption key, encrypts the decrypted packet utilizing an encryption key, and compares the encrypted result with the original encrypted packet. Daniels performs the processing to check security of data received by a computer from a client. Daniels only intends to prevent the data-security-checking software from being damaged by rejecting an incoming erroneous packet (col. 1, lines 52-59), rather than “suppressing the output for preventing an attacker from obtaining an incorrect results” as the invention. Daniels simply does not support any “tamper-resistant fault detection and which controls the output of the processing result Z to output it when it is correct”. Neither Daniels nor Fernandez suggests the purpose of tamper-resistant fault detection the present invention was designed for.

As Daniels discloses an asymmetric-key decryption process while Fernandez does a symmetric-key encryption process, Applicants contend that one skilled in the art would not be motivated to combine the teachings as suggested by the Examiner. Even if there were combined as suggested by the Examiner, the combination still fails to teach or suggest (i) outputting said processing result Z from said information processing device when said processing result W coincides with said ciphertext C ($W=C$); and (ii) suppressing the output of said processing result Z from said information processing device when said processing result W does not coincide with said ciphertext C ($W \neq C$).

Neither the cited references, nor their combinations teach or suggest each and every feature of the present invention as recited in independent claims 1 and 5. As such, the present invention as now claimed is distinguishable and thereby allowable over the rejections raised in the Office Action. The withdrawal of the outstanding prior art rejections is in order, and is respectfully solicited.

Conclusion

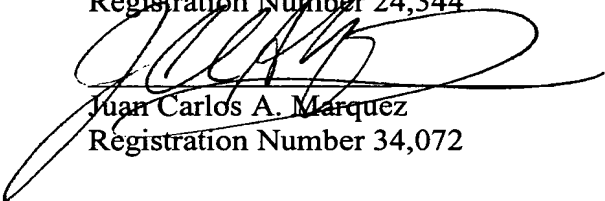
In view of all the above, Applicants respectfully submit that certain clear and distinct differences as discussed exist between the present invention as now claimed and the prior art references upon which the rejections in the Office Action rely. These differences are more

than sufficient that the present invention as now claimed would not have been anticipated nor rendered obvious given the prior art. Rather, the present invention as a whole is distinguishable, and thereby allowable over the prior art.

Favorable reconsideration of this application as amended is respectfully solicited. Should there be any outstanding issues requiring discussion that would further the prosecution and allowance of the above-captioned application, the Examiner is invited to contact the Applicant's undersigned representative at the address and phone number indicated below.

Respectfully submitted,

Stanley P. Fisher
Registration Number 24,344



Juan Carlos A. Marquez
Registration Number 34,072

REED SMITH LLP
3110 Fairview Park Drive, Suite 1400
Falls Church, Virginia 22042
(703) 641-4200

July 27, 2005

SPF/JCM/JT